计算机工程　2007 33 (06): 101-103　ISSN: 1000-3428　CN: 31-1289/TP

安全技术

基于Hash函数的报文鉴别方法

肖皇培1，张国基2

(1. 华南理工大学计算机科学与工程学院，广州 510640；2. 华南理工大学数学科学学院，广州 510640)

收稿日期　修回日期　网络版发布日期 2007-3-16　接受日期

摘要　基于当前网络通信中对报文鉴别码(MAC)的需求，介绍了Hash函数在密码学上的安全性质，分析了Hash函数在报文鉴别中的应用和针对Hash函数的主要攻击。在此基础之上，提出一种基于Hash函数的报文鉴别码——伪报文鉴别码(PMAC)。利用当前现有的Hash函数来构造MAC，而不改变原有的Hash函数的内部结构。在没有利用任何现有加密算法的基础上，仅应用一个密钥不仅对报文提供了鉴别，而且也提供了机密性。对该伪报文鉴别算法的安全性进行了初步分析。

关键词　Hash函数　报文鉴别码　伪报文鉴别码

分类号　TP393

DOI:

对应的英文版文章：2007-6-046

通讯作者:

作者个人主页: 肖皇培1;张国基2